Attorney Docket No. AT03 0055 US1 PATENT APPLICATION

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

Appellants: Ernst Haselsteiner et al. Group Art Unit: 2431

Application No.: 10/574,630 Examiner: Abrishamkar, Kaveh

Filed: May 12, 2008 Confirmation No.: 1877

For: METHOD OF AND CIRCUIT FOR IDENTIFYING
AND/OR VERIFYING HARDWARE AND/OR
SOFTWARE OF AN APPLIANCE AND OF A DATA
CARRIER COOPERATING WITH THE APPLIANCE

Mail Stop Appeal Brief-Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

APPEAL BRIEF UNDER 37 C.F.R. § 41.37(a)

This is an appeal to the Board of Patent Appeals and Interferences from the decision of the Examiner dated June 4, 2009, which finally rejected claims 1-15 in the above-identified application. The Office date of receipt of Appellants' Notice of Appeal was September 3, 2009. This Appeal Brief is hereby submitted pursuant to 37 C.F.R. § 41.37(a).

CERTIFICATE OF MAILING UNDER 37 C.F.R. 1.8
I hereby certify that this paper (along with any paper referred to as being attached or enclosed) is being facsimile transmitted to the Patent and Trademark Office on the date shown below.

Date:____________ Signed:______________________________

Typed Name: Mark A. Wilson

TABLE OF CONTENTS

I. REAL PARTY IN INTEREST 4

II. RELATED APPEALS AND INTERFERENCES 4

III. STATUS OF CLAIMS 4

IV. STATUS OF AMENDMENTS 4

V. SUMMARY OF CLAIMED SUBJECT MATTER 4

VI. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL 6

VII. ARGUMENT 6

- A. Claims 1-3 and 6 are patentable over Proudler because Proudler does not disclose all of the limitations of the claims 7
  - 1. If the request from the user of Proudler is considered to be the first authorization data, then Proudler fails to disclose comparing the first authorization data with the first verification data 11
  - 2. If the expected values, provided by the trusted party to the user, of Proudler is considered to be the first authorization data, then Proudler fails to disclose authorizing the hardware and/or software 11
  - 3. The general assertions in the rejection are insufficient to show how Proudler purportedly discloses a second unit, second authorization data, and second verification data 12
  - 4. The inconsistent assertions in the rejection are insufficient to show how Proudler purportedly discloses the first and second units 13
- B. Claim 4 is patentable over Proudler because Proudler does not disclose all of the limitations of the claim 15
- C. Claim 5 is patentable over Proudler because Proudler does not disclose all of the limitations of the claim 16

D. Claims 7, 8, and 10-15 are patentable over Proudler because Proudler does not disclose all of the limitations of the claims 16

E. Claim 9 is patentable over Proudler because Proudler does not disclose all of the limitations of the claim 18

VIII. CONCLUSION 20

IX. CLAIMS APPENDIX 21

X. EVIDENCE APPENDIX 24

XI. RELATED PROCEEDINGS APPENDIX 25

I. REAL PARTY IN INTEREST

The real party in interest is the assignee of the full interest in the invention, NXP B.V., of Eindhoven, Netherlands.

II. RELATED APPEALS AND INTERFERENCES

To the best of Appellants' knowledge, there are no appeals or interferences related to the present appeal that will directly affect, be directly affected by, or have a bearing on the Board's decision in the instant appeal.

III. STATUS OF CLAIMS

No claims are canceled.

No claims are withdrawn.

No claims are objected to.

Claims 1-15 stand rejected as follows:

Claims 1-15 stand rejected under 35 U.S.C. 102(a) as being anticipated by Proudler et al. (EP 1280042, hereinafter Proudler).

Claims 1-15 are the subject of this appeal. A copy of claims 1-15 is set forth in the Claims Appendix.

IV. STATUS OF AMENDMENTS

There were no proposed amendments submitted subsequent to the Final Office Action mailed June 4, 2009.

V. SUMMARY OF CLAIMED SUBJECT MATTER

This section of this Appeal Brief is set forth to comply with the requirements of 37 C.F.R. § 41.37(c)(1)(v) and is not intended to limit the scope of the claims in any way. Examples of implementations of the limitations of independent claims 1 and 7 and dependent claims 4, 5, and 9 are described below.

The language of claim 1 relates to a method of identifying and/or verifying hardware and/or software of an appliance and of a data carrier which is provided to cooperate with the appliance. Abstract; page 1, lines 1-2. In particular, the method includes transmitting first authorization data of the hardware and/or software to a first unit. Page 3, lines 1-3. The method also includes comparing the first authorization data of the hardware and/or software that has been transmitted to the first unit with first verification data stored in the first unit. Page 7, lines 21-23; Figure 2, step S5. The method also includes authorizing the hardware and/or software once it has been ascertained that there is coincidence between the first authorization data provided by the hardware and/or software and the first verification data stored in the first unit. Page 7, lines 24-25. The method also includes transmitting second authorization data of a data carrier to a second unit. Page 8, lines 25-27. The method also includes comparing the second authorization data in the second unit with second verification data stored in the second unit. Page 8, lines 25-27; Figure 2, step S9. The method also includes authorizing the data carrier if there is coincidence between the second authorization data and the second verification data stored in the second unit. Page 8, lines 25-29; Figure 2, step S11. The method also includes a direct data exchange carried out between the first unit and the second unit. Page 7, lines 30-33.

The language of claim 4 depends from and relates to the method of claim 1. In particular, the central arithmetic unit of the first unit and the central arithmetic unit of the second unit jointly access at least one ROM memory, one RAM memory, and/or one non-volatile memory. Page 6, lines 30-33; Figure 3.

The language of claim 5 depends from and relates to the method of claim 1. In particular, the encryption of the first authorization data and the second authorization data is carried out in the first unit and in the second unit. Page 7, lines 8-11.

The language of claim 7 relates to a circuit for identifying and/or verifying hardware and/or software of an appliance and of a data carrier which is provided to cooperate with the appliance. Page 1, lines 3-5. In particular, claim 1 recites a first unit and a second unit. The first unit identifies and/or verifies hardware and/or software of the appliance which comprises a central arithmetic unit and at least one memory and an interface to the hardware and/or software that is to be identified and/or verified. Page 6, lines 27-31; Figure 1, TPM E1, CPU 2, ROM 3, RAM 4, non-volatile memory 5, interface 7. The second unit has a central arithmetic unit and at least one memory and an interface to an external data carrier and also and interface to the hardware and/or software. Page 7, lines 8-11; Figure 1, SAM E2, CPU 10, ROM 11, RAM 12, non-volatile memory 13, interface 16, interface 17. A communication interface is provided between the central arithmetic units of the first unit and the second unit. Page 7, lines 26-29.

The language of claim 9 depends from and relates to the circuit of claim 7. In particular, the ROM memories and/or the RAM memories and/or the non-volatile memories of the first unit and of the second unit are in each case combined to form a common ROM memory and/or a common RAM memory and/or a common non-volatile memory. Figure 3, ROM 18, RAM 19, non-volatile memory 20; Page 9, lines 12-13.

VI. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

A. Whether claims 1-3 and 6 are patentable over Proudler under 35 U.S.C. 102(a).

B. Whether claim 4 is patentable over Proudler under 35 U.S.C. 102(a).

C. Whether claim 5 is patentable over Proudler under 35 U.S.C. 102(a).

D. Whether claims 7, 8, and 10-15 are patentable over Proudler under 35 U.S.C. 102(a).

E. Whether claim 9 is patentable over Proudler under 35 U.S.C. 102(a).

VII. ARGUMENT

For the purposes of this appeal, claims 1-3 and 6 are argued together as a group for purposes of the question of patentability over Proudler under 35 U.S.C. 102(a). Claim 4 is argued separately for purposes of the question of patentability over Proudler under 35 U.S.C. 102(a). Claim 5 is argued separately for purposes of the question of patentability over Proudler under 35 U.S.C. 102(a). Claims 7, 8, and 10-15 are argued as a separate group for purposes of the question of patentability over Proudler under 35 U.S.C. 102(a). Claim 9 is argued separately for purposes of the question of patentability over Proudler under 35 U.S.C. 102(a).

A. Claims 1-3 and 6 are patentable over Proudler because Proudler does not disclose all of the limitations of the claims.

Appellants respectfully submit that claim 1 is patentable over Proudler because Proudler does not disclose all the limitations of the claim. Claim 1 recites:

> A method of identifying and/or verifying hardware and/or software of an appliance and of a data carrier which is provided to cooperate with the appliance, the method comprising:
>
> transmitting first authorization data of the hardware and/or software to a first unit,
>
> comparing the first authorization data of the hardware and/or software that has been transmitted to the first unit with first verification data stored in the first unit,
>
> authorizing the hardware and/or software once it has been ascertained that there is coincidence between the first authorization data provided by the hardware and/or software and the first verification data stored in the first unit,
>
> transmitting second authorization data of a data carrier to a second unit,
>
> comparing the second authorization data in the second unit with second verification data stored in the second unit, and
>
> authorizing the data carrier if there is coincidence between the second authorization data and the second verification data stored in the second unit,
>
> wherein a direct data exchange is carried out between the first unit and the second unit.
>
> (Emphasis added.)

Hence, the claim recites several limitations, including each of the following limitations:

1. transmitting first authorization data to the first unit;
2. comparing the first authorization data with the first verification data;
3. the first verification data is stored on the first unit;
4. transmitting second authorization data to the second unit;
5. comparing the second authorization data with the second verification data; and
6. the second verification data is stored on the second unit.

Prior to discussing the deficiencies of the present rejection, it may be useful to review the actual disclosure of Proudler. In general, Proudler describes a verification process for a user to identify a trusted platform prior to exchanging other data. Proudler, col. 5, lines 28-29. The following Fig. 1 is a simplified diagram of Proudler to illustrate the pertinent interactions between the user and the trusted platform. A more detailed version of the trusted platform is shown in Fig. 6 of Proudler.

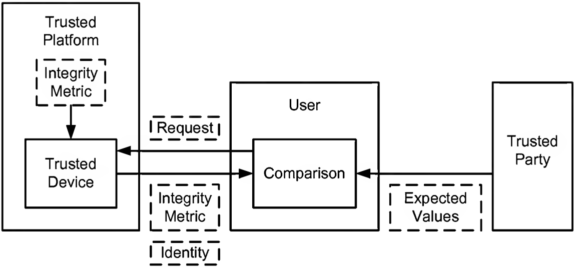

Fig. 1. Simplified illustration of the system of Proudler.

In this Fig. 1, the trusted platform includes a trusted device. The trusted device acquires an integrity metric from the trusted platform. Proudler, col. 8, lines 19-21. The integrity metric is used to indicate the state of the computing platform to the user. Proudler, col. 4, line 55, through col. 5, line 3. In particular, the user sends a request to the trusted device and, in turn, receives the proof of identity and the integrity metric. Proudler, col. 5, lines 29-35. The user then compares the received values with expected values received from a trusted party. Proudler, col. 5, lines 35-38. Once the user has established trusted operation of the platform, the user can exchange other data with the platform. Proudler, col. 5, lines 44-46.

As a more specific embodiment, Proudler indicates that the trusted platform may include a smart card reader. Proudler, Fig. 6; col. 6, lines 36-40. The smart card reader allows a user with a smart card to interact with the platform. Proudler, col. 6, lines 40-42. The following Fig. 2 illustrates a simplified diagram of this specific embodiment.

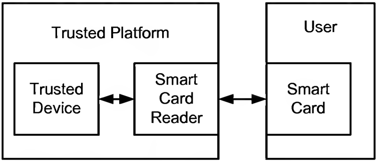

Fig. 2. Simplified illustration of a specific embodiment of the system of Proudler.

Thus, it should be understood that the smart card and the smart card reader are merely implements of the user and the platform, respectively, to allow the user and the platform to communicate with each other.

In order to understand the deficiencies of the present rejection, it may be useful to refer to the following Table 1, which attempts to correlate the asserted disclosure of Proudler with each of the foregoing limitations from claim 1.

Table 1. Correlation between some claim limitations and the asserted disclosure of Proudler.

Claim Limitation	Disclosure of Proudler
"transmitting first authorization data to the first unit"	The user sends a nonce (e.g., random number) to the trusted device and receives a response used to verify the trusted device (paragraphs 16-19, 29-30, 41, and 49-51). Office Action, 6/4/09, page 4.
"comparing the first authorization data with the first verification data"	The identity and integrity metric of the trusted device are compared with expected values provided by a trusted party (paragraph 16). Office Action, 6/4/09, page 4.
	The first verification data is viewed as the integrity metric which is shown to authenticate the trusted platform (paragraph 29). Office Action, 6/4/09, page 2

	(repeated in the Advisory Action).
"storing first verification data on the first unit"	The identity and integrity metric of the trusted device are compared with expected values provided by a trusted party (paragraph 16). Office Action, 6/4/09, page 4.
"transmitting second authorization data to the second unit"	Verification between a smart card and a trusted device (paragraph 22, 29, 44). Office Action, 6/4/09, page 4.
"comparing the second authorization data with the second verification data"	Verification between a smart card and a trusted device (paragraph 22, 29, 44). Office Action, 6/4/09, page 4.
"the second verification data is stored on the second unit"	Verification between a smart card and a trusted device (paragraph 22, 29, 44). Office Action, 6/4/09, page 4.

In considering the assertions regarding the first three limitations included in Table 1 above, related to the first unit, first authorization data, and first verification data, there appear to be two possible interpretations asserted by the Examiner. The first interpretation relies on a correspondence between the nonce of Proudler and the first authorization data recited in the claim. The second interpretation relies on a correspondence between the expected values of Proudler (delivered from the Trusted Party to the user) and the first authorization data recited in the claim. However, both of these possible assertions are insufficient to address all of the limitations related to the first unit, first authorization data, and first verification data. Furthermore, in considering the assertions regarding the last three limitations in Table 1, related to the second unit, second authorization data, and second verification data, the reasoning presented in the Office Action fails to show how Proudler purportedly discloses all of these limitations. Additionally, the reasoning in the Office Action is inconsistent in its designation of structures within Proudler that purportedly disclose the first and second units. These discrepancies are sufficient to provide multiple reasons for withdrawal of the rejection of claim 1, as explained below.

1. If the request from the user of Proudler is considered to be the first authorization data, then Proudler fails to disclose comparing the first authorization data with the first verification data.

One possible interpretation of the assertions in the Office Action relies on a correspondence between the request from the user of Proudler and the first authorization data recited in the claim. It should be noted that this does not appear to be the intent of the Examiner; however, this analysis is provided for the sake addressing the various facets of the rejection, in its entirety.

In the event that the rejection relies on the request from the user to the trusted party as the first authorization data, Proudler fails to disclose comparing the request to first verification data. Specifically, Proudler does not describe any type of comparison operations to compare the request from the user to the trusted device with another parameter. Therefore, even if the Examiner intended to draw a relationship between the request from the user and the first authorization data recited in the claim, such relationship nevertheless fails to satisfy the limitation that the first authorization data is compared with the first verification data.

2. If the expected values, provided by the trusted party to the user, of Proudler are considered to be the first authorization data, then Proudler fails to disclose authorizing the hardware and/or software.

The other possible interpretation of the assertions in the Office Action relies on a correspondence between the expected values (sent from the trusted party to the user) of Proudler and the first authorization data. This appears to be the interpretation intended by the Examiner. However, this interpretation also fails to disclose all of the limitations of the claim.

To properly understand the deficiency of this interpretation, it should be noted that the claim recites transmitting the first authorization data of the hardware and/or software to the first unit. Thus, if the expected values are interpreted as the first authorization data, then the trusted party must be interpreted as the hardware and/or software, and the user must be interpreted as the first unit. For reference, these necessary correlations are summarized in the following Table 2:

Table 2. Correlation between claim limitations
and the disclosure of Proudler.

Claim Limitation	Disclosure of Proudler
First Authorization Data	Expected Values
Hardware and/or Software	Trusted Party
First Unit	User

However, these correlations are nevertheless insufficient to disclose "authorizing the hardware and/or software once it has been ascertained that there is coincidence between the first authorization data provided by the hardware and/or software and the first verification data stored in the first unit" (emphasis added), as recited in the claim. In other words, there is no disclosure of authorizing the trusted party, which under this interpretation would necessarily correlate to the hardware and/or software recited in the claim. Since there is no disclosure of authorizing the trusted party, this interpretation fails to disclose authorizing the hardware and/or software. Accordingly, this interpretation also fails to disclose all of the limitations of the claim.

3. The general assertions in the rejection are insufficient to show how Proudler purportedly discloses a second unit, second authorization data, and second verification data.

As a separate basis for patentability, the reasoning in the Office Action merely refers to general descriptions of the verification process between a smart card and a trusted device. However, even if the transmission disclosed by Proudler were considered to be first authorization and verification data, such general descriptions of the verification process are insufficient to specifically disclose second authorization and verification data. Rather, the indicated descriptions of smart card verification merely address a specific implementation of the more general embodiment which refers generally to the platform/device and the user, rather than specifically to the smart card reader and the smart card. Thus, as shown in the illustration of Fig. 2 above, the use of the smart card reader and the smart card is merely a specific implementation of the platform and the user shown in the illustration of Fig. 1 above.

Since the smart card reader is merely a component of one implementation of the trusted platform, it would not be logical to assert that the smart card reader might be a separate unit from the trusted platform. Similarly, since the smart card is merely a component of one implementation of the user, it would not be logical to assert that the smart card might be a separate unit from the user. Therefore, the disclosure of a specific embodiment which includes the smart card reader and the smart card should be interpreted as a disclosure of units and/or data that are separate from the more general embodiments of the platform and the user.

Hence, the reasoning in the rejection should not attempt to rely on the general embodiments of the platform and the user as disclosing the first unit and the first authorization/verification data, while asserting that the more specific embodiment of the smart card reader and the smart card purportedly disclose the second unit and the second authorization/verification data. In reality, these general and specific embodiments merely relate to the same components and data operations, so they should not be misconstrued as disclosing separate components or data operations.

For the reasons presented above, Proudler does not disclose all of the limitations of the claim because Proudler does not disclose both first authorization data and verification data stored on a first unit and second authorization data and verification data stored on a second unit, as recited in the claim. Rather, Proudler merely describes general and specific embodiments of the same components and data operations. Accordingly, Appellants respectfully assert claim 1 is patentable over Proudler because Proudler does not disclose all of the limitations of the claim.

4. The inconsistent assertions in the rejection are insufficient to show how Proudler purportedly discloses the first and second units.

As a separate basis for patentability, the reasoning in the Office Action is inconsistent and, hence, is not sufficient to show how Proudler purportedly discloses the first and second units recited in the claim. As explained above, the reasoning in the Office Action leaves open the possibilities that either the trusted device or the user is asserted as the first unit recited in the claim. Also, the reasoning in the Office Action clearly relies on either the trusted device or the smart card (of the user) as the second unit, according to the last three limitations listed in Table 1 above. Thus, these interpretations appear to rely solely on the trusted device and the user (either generally or specifically in the form of the smart card) as the first and second units recited in the claim.

However, the reasoning in the Office Action inconsistently refers to the trusted device and the trusted platform as the first and second units, in conjunction with the claim language related to a direct data exchange carried out between the first unit and the second unit. In other words, this portion of the rejection relies on the trusted platform as one of the first and second units, even though the trusted device is part of the trusted platform (see Fig. 6 of Proudler) and the other reasoning in the rejection only relies on either the trusted device or the user as the first and second units.

In light of this inconsistency in the reasoning of the present rejection, the rejection must be insufficient to show how Proudler purportedly discloses all of the limitations of the claims because Proudler, at best, might disclose some but not all of the limitations of the claim. Specifically, if the trusted device and the user are construed as the first and second units, then Proudler fails to disclose a direct data exchange carried out between the first and second units. On the other hand, if the trusted device and the trusted platform are construed as the first and second units with respect to the direct data exchange, as asserted in the Office Action, then Proudler fails to disclose all of the other limitations which rely on an incompatible interpretation with the trusted device and the user as the first and second units. Therefore, in either case, there must be some limitations of the claim that are not disclosed by Proudler because the inconsistent assertions in the Office Action necessarily conflict and cannot both be asserted.

Given that claims 2-6 depend from and incorporate all of the limitations of independent claim 1, which is patentable over the cited references, Appellants respectfully submit that these claims are also patentable over the cited reference based on an allowable base claim. Additionally, each of these claims may be allowable for further reasons. Accordingly, Appellants request that the rejections of claims 2-6 under 35 U.S.C. 102(a) be withdrawn.

B. Claim 4 is patentable over Proudler because Proudler does not disclose all of the limitations of the claim.

Given that claim 4 depends from and incorporates all of the limitations of independent claim 1, which is patentable over Proudler, Appellants respectfully submit that dependent claim 4 is also patentable over Proudler based on an allowable base claim. Additionally, claim 4 is patentable over Proudler for further reasons, as explained below.

Additionally, Appellants respectfully submit that claim 4 is patentable over Proudler because Proudler does not disclose all the limitations of the claim. Claim 4 recites:

> A method as claimed in claim 1, wherein a central arithmetic unit of the first unit and a central arithmetic unit of the second unit jointly access at least one ROM memory one RAM memory and/or one non-volatile memory.

(Emphasis added.)

In contrast, Proudler does not disclose multiple central arithmetic units that jointly access memory, at least because Proudler does not disclose multiple central arithmetic units of first and second units. Moreover, even if Proudler were to describe multiple central arithmetic units, Proudler does not describe multiple central arithmetic units jointly accessing a memory device. In other words, there is no description in Proudler of a memory that is jointly accessed by multiple central arithmetic units. Even though the Examiner cites the measurement function of Proudler, the measurement function disclosed in Proudler does not describe multiple central arithmetic units from the first and second unit each jointly accessing a memory. Therefore, Proudler does not disclose all of the limitations of the claim because Proudler does not disclose multiple central arithmetic units jointly accessing memory, as recited in the claim. Accordingly, Appellants respectfully assert claim 4 is patentable over Proudler because Proudler does not disclose all of the limitations of the claim.

C. Claim 5 is patentable over Proudler because Proudler does not disclose all of the limitations of the claim.

Given that claim 5 depends from and incorporates all of the limitations of independent claim 1, which is patentable over Proudler, Appellants respectfully submit that dependent claim 5 is also patentable over Proudler based on an allowable base claim. Additionally, claim 5 is patentable over Proudler for further reasons, as explained below.

Additionally, Appellants respectfully submit that claim 5 is patentable over Proudler because Proudler does not disclose all the limitations of the claim. Claim 5 recites:

> A method as claimed in claim 1, wherein encryption of the first authorization data and of the second authorization data is carried out in the first unit and in the second unit.
>
> (Emphasis added.)

In contrast, Proudler does not disclose encryption of first and second authorization data, at least because Proudler does not disclose both first and second authorization data, as explained above with respect to the rejection of claim 1. Therefore, Proudler does not disclose all of the limitations of the claim because Proudler does not disclose encrypting both first and second authorization data, as recited in the claim. Even though the Examiner broadly cites "paragraph 0019, paragraph 0051: cryptographic processes," the Examiner fails to provide any reasoning or support in the purported rejection of claim 5 because the cited portions of Proudler do not disclose encrypting both first and second authorization data, as recited in the claim. Accordingly, Appellants respectfully assert claim 5 is patentable over Proudler because Proudler does not disclose all of the limitations of the claim.

D. Claims 7, 8, and 10-15 are patentable over Proudler because Proudler does not disclose all of the limitations of the claims.

Appellants respectfully submit that claim 7 is patentable over Proudler because Proudler does not disclose all the limitations of the claim. Claim 7 recites:

> A circuit for identifying and/or verifying hardware and/or software of an appliance and of a data carrier which is provided to cooperate with the appliance, the circuit comprising:
>
> a first unit for identifying and/or verifying the hardware and/or software of the appliance, comprising a central arithmetic unit and at least one memory and an interface to the hardware and/or software that is to be identified and/or verified, and
>
> a second unit comprising a central arithmetic unit and at least one memory and an interface to an external data carrier and also an interface to the hardware and/or software,
>
> wherein a communication interface is provided between the central arithmetic units of the first unit and the second unit.

(Emphasis added.)

In contrast, Proudler does not disclose separate units each with a separate central arithmetic unit and at least one memory. Rather, Proudler merely describes a trusted device 24 and a smart card reader 12 within a trusted platform 10. Proudler, Fig. 6. Although Proudler describes the trusted device 24 as including a controller 30 and memory 3 and 4 (Proudler, Fig. 8), Proudler does not describe any components within the smart card reader 12. Furthermore, the components of the trusted device 24 should not be construed as a central arithmetic unit or memory of the smart card reader 12 because Proudler does not describe the smart card reader 12 having access to the components of the trusted device 24.

In support of the rejection, the Examiner asserts that:

> It is well-known in the art that a smart card reader has an arithmetic unit for calculating and comparing authentication data.

Office Action, 6/4/2009, pages 2-3.

However, the Office Action does not offer any support or reasoning for this assertion. Moreover, the assertion of a "well-known" teaching is inappropriate to establish actual disclosure, as required for a rejection under 35 U.S.C. 102.

Moreover, Proudler is clear in the disclosure of a single main processor (Proudler, paragraphs 23-26; and Fig. 7, main processor 21) to drive the processes of the trusted platform. Therefore, the assertion that the reader of Proudler purportedly includes an arithmetic unit is unfounded and unsupported by the prior art. Furthermore, Proudler does not describe the smart card reader 12 as sharing or even having access to the main processor 21 or the memory 22 of the motherboard 20. Therefore, the components of the motherboard 20 should not be construed as a central arithmetic unit or memory of the smart card reader 12 because Proudler does not describe the smart card reader 12 having access to the components of the motherboard 20. Therefore, Proudler does not describe multiple units that each includes a central arithmetic unit and at least one memory, as recited in the claim.

For the reasons presented above, Proudler does not disclose all of the limitations of the claim because Proudler does not disclose first and second units that each include a central arithmetic unit and at least one memory, as recited in the claim. Accordingly, Appellants respectfully assert claim 7 is patentable over Proudler because Proudler does not disclose all of the limitations of the claim.

Given that claims 8-15 depend from and incorporate all of the limitations of independent claim 7, which is patentable over the cited references, Appellants respectfully submit that these claims are also patentable over the cited reference based on an allowable base claim. Additionally, each of these claims may be allowable for further reasons. Accordingly, Appellants request that the rejections of claims 7-15 under 35 U.S.C. 102(a) be withdrawn.

E. Claim 9 is patentable over Proudler because Proudler does not disclose all of the limitations of the claim.

Given that claim 9 depends from and incorporates all of the limitations of independent claim 7, which is patentable over Proudler, Appellants respectfully submit that dependent claim 9 is also patentable over Proudler based on an allowable base claim. Additionally, claim 9 is patentable over Proudler for further reasons, as explained below.

Additionally, Appellants respectfully submit that claim 9 is patentable over Proudler because Proudler does not disclose all the limitations of the claim. Claim 9 recites:

> A circuit as claimed in claim 7, wherein the ROM memories and/or the RAM memories and/or the non-volatile memories of the first unit and of the second unit are in each case combined to form a common ROM memory and/or a common RAM memory and/or a common non-volatile memory.

(Emphasis added.)

Appellants respectfully assert claim 9 is patentable over Proudler at least for similar reasons to those stated above in regard to the rejection of claim 4. Here, although the language of claim 9 differs from the language of claim 4, and the scope of claim 9 should be interpreted independently of claim 4, Appellants respectfully assert that the remarks provided above in regard to the rejection of claim 4 also apply to the rejection of claim 9. As explained above, Proudler does not describe a common memory that is jointly accessed by first and second units. Even though the Examiner repeats the citation used with regard to claim 4, the measurement function disclosed in Proudler does not describe memory units from the first and second unit combined to jointly form a common memory. Accordingly, Appellants respectfully assert claim 9 is patentable over Proudler because Proudler does not disclose a common memory.

VIII. CONCLUSION

For the reasons stated above, claims 1-15 are patentable over the cited references. Thus, the rejections of claims 1-15 should be withdrawn. Appellants respectfully request that the Board reverse the rejections of claims 1-15 under 35 U.S.C. 102 (a) and, since there are no remaining grounds of rejection to be overcome, direct the Examiner to enter a Notice of Allowance for claims 1-15.

At any time during the pendency of this application, please charge any fees required or credit any over payment to Deposit Account **50-4019** pursuant to 37 C.F.R. 1.25. Additionally, please charge any fees to Deposit Account **50-4019** under 37 C.F.R. 1.16, 1.17, 1.19, 1.20 and 1.21.

Respectfully submitted,

/mark a. wilson/

Date: November 2, 2009

Mark A. Wilson
Reg. No. 43,994

Wilson & Ham
PMB: 348
2530 Berryessa Road
San Jose, CA 95132
Phone: (925) 249-1300
Fax: (925) 249-0111

IX. CLAIMS APPENDIX

1. A method of identifying and/or verifying hardware and/or software of an appliance and of a data carrier which is provided to cooperate with the appliance, the method comprising:

transmitting first authorization data of the hardware and/or software to a first unit,

comparing the first authorization data of the hardware and/or software that has been transmitted to the first unit with first verification data stored in the first unit,

authorizing the hardware and/or software once it has been ascertained that there is coincidence between the first authorization data provided by the hardware and/or software and the first verification data stored in the first unit,

transmitting second authorization data of a data carrier to a second unit,

comparing the second authorization data in the second unit with second verification data stored in the second unit, and

authorizing the data carrier if there is coincidence between the second authorization data and the second verification data stored in the second unit,

wherein a direct data exchange is carried out between the first unit and the second unit.

2. A method as claimed in claim 1, wherein the direct data exchange between the first unit and the second unit comprises a transmission of encrypted data and a comparison and/or decryption of data transmitted between the first unit and the second unit.

3. A method as claimed in claim 1, wherein the data exchange between the first unit and the second unit is carried out prior to an identification and/or verification of first authorization data of the hardware and/or software and of second authorization data of the data carrier.

4. A method as claimed in claim 1, wherein a central arithmetic unit of the first unit and a central arithmetic unit of the second unit jointly access at least one ROM memory one RAM memory and/or one non-volatile memory.

5. A method as claimed in claim 1, wherein encryption of the first authorization data and of the second authorization data is carried out in the first unit and in the second unit.

6. A method as claimed in claim 1, wherein the second authorization data are obtained from a smartcard or a tag or a label that forms the data carrier.

7. A circuit for identifying and/or verifying hardware and/or software of an appliance and of a data carrier which is provided to cooperate with the appliance, the circuit comprising:

a first unit for identifying and/or verifying the hardware and/or software of the appliance, comprising a central arithmetic unit and at least one memory and an interface to the hardware and/or software that is to be identified and/or verified, and

a second unit comprising a central arithmetic unit and at least one memory and an interface to an external data carrier and also an interface to the hardware and/or software,

wherein a communication interface is provided between the central arithmetic units of the first unit and the second unit.

8. A circuit as claimed in claim 7, wherein the memories of the first unit and of the second unit are formed by a ROM memory and a RAM memory and/or a non-volatile memory.

9. A circuit as claimed in claim 7, wherein the ROM memories and/or the RAM memories and/or the non-volatile memories of the first unit and of the second unit are in each case combined to form a common ROM memory and/or a common RAM memory and/or a common non-volatile memory.

10. A circuit as claimed in claim 7, wherein the first unit and the second unit in each case comprise an encryption device.

11. A circuit as claimed in claim 7, wherein the central arithmetic unit of the first unit and the central arithmetic unit of the second unit are combined to form a common central arithmetic unit which common central arithmetic unit has the integrated communication interface, and wherein the common central arithmetic unit is connected by an interface to the hardware and/or software that is to be identified and/or verified.

12. A circuit as claimed in claim 7, wherein the interface to the external data carrier is designed for contactless communication with the external data carrier.

13. A circuit as claimed in claim 7, wherein the external data carrier is formed by a smartcard or a tag or a label.

14. An appliance which comprises as hardware at least one central arithmetic unit which central arithmetic unit is designed to run software and to obtain data from an external data carrier cooperating with the appliance, wherein a circuit as claimed in claim 7 is coupled to the central arithmetic unit.

15. An appliance as claimed in claim 14, wherein the central arithmetic unit of the appliance is coupled via an interface integrated in the central arithmetic unit of the appliance to the circuit integrated in the central arithmetic unit.

X. EVIDENCE APPENDIX

There is no evidence submitted with this Appeal Brief.

XI. RELATED PROCEEDINGS APPENDIX

To the best of Appellants' knowledge, there are no appeals or interferences related to the present appeal that will directly affect, be directly affected by, or have a bearing on the Board's decision in the instant appeal.